

计算机网络基础知识总结

1. 网络层次划分

2. OSI 七层网络模型

3. IP 地址

4. 子网掩码及网络划分

5. ARP/RARP 协议

6. 路由选择协议

7. TCP/IP 协议

8. UDP 协议

9. DNS 协议

10. NAT 协议

11. DHCP 协议

12. HTTP 协议

13. 一个举例

计算机网络学习的核心内容就是网络协议的学习。网络协议是为计算机网络中进行数据交换而建立的规则、标准或者说是约定的集合。因为不同用户的数据终端可能采取的字符集是不同的，两者需要进行通信，必须要在一定的标准上进行。一个很形象地比喻就是我们的语言，我们大天朝地广人多，地方性语言也非常丰富，而且方言之间差距巨大。A 地区的方言可能 B 地区的人根本无法接受，所以我们要为全国人名进行沟通建立一个语言标准，这就是我们的普通话的作

用。同样，放眼全球，我们与外国友人沟通的标准语言是英语，所以我们才要苦逼的学习英语。

计算机网络协议同我们的语言一样，多种多样。而 ARPA 公司于 1977 年到 1979 年推出了一种名为 ARPANET 的网络协议受到了广泛的热捧，其中最主要的原因就是它推出了人尽皆知的 TCP/IP 标准网络协议。目前 TCP/IP 协议已经成为 Internet 中的“通用语言”，下图为不同计算机群之间利用 TCP/IP 进行通信的示意图。

1. 网络层次划分

为了使不同计算机厂家生产的计算机能够相互通信，以便在更大的范围内建立计算机网络，国际标准化组织（ISO）在 1978 年提出了“开放系统互联参考模型”，即著名的 OSI/RM 模型（Open System Interconnection/Reference Model）。它将计算机网络体系结构的通信协议划分为七层，自下而上依次为：物理层（Physics Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）、应用层（Application Layer）。其中第四层完成数据传送服务，上面三层面向用户。

除了标准的 OSI 七层模型以外，常见的网络层次划分还有 TCP/IP 四层协议以及 TCP/IP 五层协议，它们之间的对应关系如下图所示：

2. OSI 七层网络模型

TCP/IP 协议毫无疑问是互联网的基础协议，没有它就根本不可能上网，任何和互联网有关的操作都离不开 TCP/IP 协议。不管是 OSI 七层模型还是 TCP/IP

的四层、五层模型，每一层中都要自己的专属协议，完成自己相应的工作以及与上下层级之间进行沟通。由于 OSI 七层模型为网络的标准层次划分，所以我们可以 OSI 七层模型为例从下向上进行一一介绍。

1) 物理层 (Physical Layer)

激活、维持、关闭通信端点之间的机械特性、电气特性、功能特性以及过程特性。该层为上层协议提供了一个传输数据的可靠的物理媒体。简单的说，物理层确保原始的数据可在各种物理媒体上传输。物理层记住两个重要的设备名称，中继器 (Repeater，也叫放大器) 和集线器。

2) 数据链路层 (Data Link Layer)

数据链路层在物理层提供的服务的基础上向网络层提供服务，其最基本的服务是将源自网络层来的数据可靠地传输到相邻节点的目标机网络层。为达到这一目的，数据链路必须具备一系列相应的功能，主要有：如何将数据组合成数据块，在数据链路层中称这种数据块为帧 (frame)，帧是数据链路层的传送单位；如何控制帧在物理信道上的传输，包括如何处理传输差错，如何调节发送速率以使与接收方相匹配；以及在两个网络实体之间提供数据链路通路的建立、维持和释放的管理。数据链路层在不可靠的物理介质上提供可靠的传输。该层的作用包括：物理地址寻址、数据的成帧、流量控制、数据的检错、重发等。

有关数据链路层的重要知识点：

1> 数据链路层为网络层提供可靠的数据传输；

2> 基本数据单位为帧；

3> 主要的协议：以太网协议；

4> 两个重要设备名称：网桥和交换机。

3) 网络层 (Network Layer)

网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括寻址和路由选择、连接的建立、保持和终止等。它提供的服务使传输层不需要了解网络中的数据交换技术。如果您想用尽量少的词来记住网络层，那就是“路径选择、路由及逻辑寻址”。

网络层中涉及众多的协议，其中包括最重要的协议，也是 TCP/IP 的核心协议——IP 协议。IP 协议非常简单，仅提供不可靠、无连接的传送服务。IP 协议的主要功能有：无连接数据报传输、数据报路由选择和差错控制。与 IP 协议配套使用实现其功能的还有地址解析协议 ARP、逆地址解析协议 RARP、因特网报文协议 ICMP、因特网组管理协议 IGMP。具体的协议我们会在接下来的部分进行总结，有关网络层的重点为：

1> 网络层负责对子网间的数据包进行路由选择。此外，网络层还可以实现拥塞控制、网际互连等功能；

2> 基本数据单位为 IP 数据报；

3> 包含的主要协议：

IP 协议 (Internet Protocol, 因特网互联协议) ；

ICMP 协议 (Internet Control Message Protocol, 因特网控制报文协议) ；

ARP 协议 (Address Resolution Protocol , 地址解析协议) ;

RARP 协议 (Reverse Address Resolution Protocol , 逆地址解析协议)。

4> 重要的设备：路由器。

4) 传输层 (Transport Layer)

第一个端到端，即主机到主机的层次。传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输。此外，传输层还要处理端到端的差错控制和流量控制问题。

传输层的任务是根据通信子网的特性，最佳的利用网络资源，为两个端系统的会话层之间，提供建立、维护和取消传输连接的功能，负责端到端的可靠数据传输。在这一层，信息传送的协议数据单元称为段或报文。

网络层只是根据网络地址将源结点发出的数据包传送到目的结点，而传输层则负责将数据可靠地传送到相应的端口。

有关网络层的重点：

1> 传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输以及端到端的差错控制和流量控制问题；

2> 包含的主要协议：TCP 协议 (Transmission Control Protocol , 传输控制协议)、UDP 协议 (User Datagram Protocol , 用户数据报协议)；

3> 重要设备：网关。

5) 会话层

会话层管理主机之间的会话进程，即负责建立、管理、终止进程之间的会话。
会话层还利用在数据中插入校验点来实现数据的同步。

6) 表示层

表示层对上层数据或信息进行变换以保证一个主机应用层信息可以被另一个主机的应用程序理解。表示层的数据转换包括数据的加密、压缩、格式转换等。

7) 应用层

为操作系统或网络应用程序提供访问网络服务的接口。

会话层、表示层和应用层重点：

- 1) 数据传输基本单位为报文；
- 2) 包含的主要协议：FTP（文件传送协议）、Telnet（远程登录协议）、DNS（域名解析协议）、SMTP（邮件传送协议），POP3 协议（邮局协议），HTTP 协议（Hyper Text Transfer Protocol）。

3. IP地址

1) 网络地址

IP 地址由网络号（包括子网号）和主机号组成，网络地址的主机号为全 0，网络地址代表着整个网络。

2) 广播地址

广播地址通常称为直接广播地址，是为了区分受限广播地址。

广播地址与网络地址的主机号正好相反，广播地址中，主机号为全 1。当向某个网络的广播地址发送消息时，该网络内的所有主机都能收到该广播消息。

3) 组播地址

D 类地址就是组播地址。

先回忆下 A, B, C, D 类地址吧：

A 类地址以 00 开头，第一个字节作为网络号，地址范围为： ；

B 类地址以 10 开头，前两个字节作为网络号，地址范围是： C 类地址以 110 开头，前三个字节作为网络号，地址范围是： 。

D 类地址以 1110 开头，地址范围是，D 类地址作为组播地址（一对多的通信）；

E 类地址以 1111 开头，地址范围是，E 类地址为保留地址，供以后使用。

注：只有 A, B, C 有网络号和主机号之分，D 类地址和 E 类地址没有划分网络号和主机号。

4) 该 IP 地址指的是受限的广播地址。受限广播地址与一般广播地址（直接广播地址）的区别在于，受限广播地址只能用于本地网络，路由器不会转发以受限广播地址为目的地址的分组；一般广播地址既可在本地广播，也可跨网段广播。例如：主机上的直接广播数据包后，另外一个网段也能收到该数据报；若发送受限广播数据报，则不能收到。

注：一般的广播地址（直接广播地址）能够通过某些路由器（当然不是所有的路由器），而受限的广播地址不能通过路由器。

5) 常用于寻找自己的 IP 地址,例如在我们的 RARP ,BOOTP 和 DHCP 协议中,若某个未知 IP 地址的无盘机想要知道自己的 IP 地址,它就以为目的地址,向本地范围(具体而言是被各个路由器屏蔽的范围内)的服务器发送 IP 请求分组。

6) 回环地址

被用作回环地址,回环地址表示本机的地址,常用于对本机的测试,用的最多的是。

7) A、B、C 类私有地址

私有地址(private address)也叫专用地址,它们不会在全球使用,只具有本地意义。

A 类私有地址: , 范围是: B 类私有地址: , 范围是: C 类私有地址: , 范围是: 子网掩码及网络划分

随着互连网应用的不断扩大,原先的 IPv4 的弊端也逐渐暴露出来,即网络号占位太多,而主机号位太少,所以其能提供的主机地址也越来越稀缺,目前除了使用 NAT 在企业内部利用保留地址自行分配以外,通常都对一个高类别的 IP 地址进行再划分,以形成多个子网,提供给不同规模的用户群使用。

这里主要是为了在网络分段情况下有效地利用 IP 地址,通过对主机号的高位部分取作为子网号,从通常的网络位界限中扩展或压缩子网掩码,用来创建某类地址的更多子网。但创建更多的子网时,在每个子网上的可用主机地址数目会比原先减少。

什么是子网掩码

子网掩码是标志两个 IP 地址是否同属于一个子网的，也是 32 位二进制地址，其每一个为 1 代表该位是网络位，为 0 代表主机位。它和 IP 地址一样也是使用点式十进制来表示的。如果两个 IP 地址在子网掩码的按位与的计算下所得结果相同，即表明它们共属于同一子网中。

在计算子网掩码时，我们要注意 IP 地址中的保留地址，即“0”地址和广播地址，它们是指主机地址或网络地址全为“0”或“1”时的 IP 地址，它们代表着本网络地址和广播地址，一般是不能被计算在内的。

子网掩码的计算：

对于无须再划分成子网的 IP 地址来说，其子网掩码非常简单，即按照其定义即可写出：如某 B 类 IP 地址为 ，无须再分割子网，则该 IP 地址的子网掩码。如果它是一个 C 类地址，则其子网掩码为 。其它类推，不再详述。下面我们关键要介绍的是一个 IP 地址，还需要将其高位主机位再作为划分出的子网网络号，剩下的是每个子网的主机号，这时该如何进行每个子网的掩码计算。

下面总结一下有关子网掩码和网络划分常见的面试题：

1) 利用子网数来计算

在求子网掩码之前必须先搞清楚要划分的子网数目，以及每个子网内的所需主机数目。

(1) 将子网数目转化为二进制来表示；

如欲将 B 类 IP 地址划分成 27 个子网：27=11011 ；

(2) 取得该二进制的位数，为 N ；

该二进制为五位数， $N = 5$

(3) 取得该 IP 地址的类子网掩码，将其主机地址部分的的前 N 位置 1 即得出该 IP 地址划分子网的子网掩码。

将 B 类地址的子网掩码的主机地址前 5 位置 1，得到 2) 利用主机数来计算

如欲将 B 类 IP 地址划分成若干子网，每个子网内有主机 700 台：

(1) 将主机数目转化为二进制来表示；

$700 = 1010110100$ ；

(2) 如果主机数小于或等于 254（注意去掉保留的两个 IP 地址），则取得该主机的二进制位数，为 N ，这里肯定 $N < 8$ 。如果大于 254，则 $N > 8$ ，这就是说主机地址将占据不止 8 位；

该二进制为十位数， $N = 10$ ；

(3) 使用来将该类 IP 地址的主机地址位数全部置 1，然后从后向前的将 N 位全部置为 0，即为子网掩码值。

将该 B 类地址的子网掩码的主机地址全部置 1，得到，然后再从后向前将后 10 位置 0，即为： $\dots 00000000$ ，即。这就是该欲划分成主机为 700 台的 B 类 IP 地址 的子网掩码。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/14807210065007004>